

Implementing the Deutsch-Jozsa algorithm with macroscopic ensembles

Henry Semenenko^{1,2} and Tim Byrnes^{3,4,5}

¹*The University of Nottingham, University Park, Nottingham, NG7 2RD, UK*

²*The University of Bristol, Senate House, Tyndall Avenue, Bristol, BS8 1TH, UK*

³*New York University, 1555 Century Ave, Pudong, Shanghai 200122, China*

⁴*NYU-ECNU Institute of Physics at NYU Shanghai,
3663 Zhongshan Road North, Shanghai 200062, China*

⁵*National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*
(Dated: May 2, 2016)

Quantum computing implementations under consideration today typically deal with systems with microscopic degrees of freedom such as photons, ions, cold atoms, and superconducting circuits. The quantum information is stored typically in low-dimensional Hilbert spaces such as qubits, as quantum effects are strongest in such systems. It has however been demonstrated that quantum effects can be observed in mesoscopic and macroscopic systems, such as nanomechanical systems and gas ensembles. While few-qubit quantum information demonstrations have been performed with such macroscopic systems, a quantum algorithm showing exponential speedup over classical algorithms is yet to be shown. Here we show that the Deutsch-Jozsa algorithm can be implemented with macroscopic ensembles. The encoding that we use avoids the detrimental effects of decoherence that normally plagues macroscopic implementations. We discuss two mapping procedures which can be chosen depending upon the constraints of the oracle and the experiment. Both methods have an exponential speedup over the classical case, and only require control of the ensembles at the level of the total spin of the ensembles. It is shown that both approaches reproduce the qubit Deutsch-Jozsa algorithm, and are robust under decoherence.

PACS numbers: 03.75.Gg, 03.75.Mn, 42.50.Gy, 03.67.Hk

I. INTRODUCTION

In 1985, David Deutsch provided the first quantum algorithm that showed the potential for quantum computing to be more powerful than classical computing – Deutsch’s algorithm [1]. It was later expanded upon by Richard Jozsa [2], and improved by Cleve, Ekert, Macchiavello and Masca [3], resulting in the multi-qubit generalization known today as Deutsch-Jozsa algorithm. One of the key features of the algorithm is that creates a superposition of all possible states, then is followed by an interference and measurement step – a key component of many quantum algorithms. It therefore paved the way for other more practical quantum algorithms such as Grover’s algorithm [4] and Shor’s algorithm [5], both of which provide a quantum mechanical speedup over the best available classical algorithms. For this reason the algorithm remains important from a theoretical point of view of the power of quantum computing, and from an experimental point of view as a proof-of-principle operation of quantum computer prototypes. Examples of experimental demonstration of Deutsch-Jozsa algorithm include NMR [6, 7], superconducting qubits [8], single photon linear optics [9], and trapped ions [10]. Currently demonstrations of quantum algorithms are typically limited to $\lesssim 10$ qubits, due to limitations with decoherence and scalability of current quantum computing technologies.

To implement a given quantum algorithm, currently there are two main paradigms of quantum computation, using either discrete or continuous variables (CV). The

most commonly used approach uses discrete quantum states to encode quantum information, typically in the form of qubits. Alternatively, one may store quantum information in a bosonic mode which has an infinite Hilbert space dimension, and states can be visualized in the phase space of position and momentum [11]. An equivalent approach involves using total spin operators as quasi-bosonic variables to implement CV [12, 13]. Recently, a third alternative to these paradigms has emerged [14, 15], having characteristics common to both. The scheme – which we call ensemble quantum computation (EQC) – stores quantum information on ensembles of qubits and manipulates them using only products of total spin operators. While it has been known for some time that it is possible to form continuous variable bosonic mode operators using polarized spins, the scheme differs from this by the full use of the space of states available on the Bloch sphere. For continuous variables implementations typically the spins are polarized in the S^X direction and only small deviations from this are induced. The scheme has the advantage that it has the same Bloch sphere structure as is the case with standard qubits, yet with a natural robustness due to the use of ensembles instead of single qubits. As the states that are used are not explicitly gaussian in a CV sense, many of the no-go results for continuous variables do not immediately apply, making non-trivial operations possible with low order products of spin operators. Indeed, it has been shown that universal operations are possible with products of one and two total spin operators [15].

One of the difficulties with EQC is that it is not always straightforward to translate a qubit or CV quantum al-

gorithm into that with ensembles. Part of the difficulty here is that due to the large Hilbert space available to the ensemble as compared to the original qubit circuit, the mapping is not unique. Thus there is a great amount of freedom in choosing the best encoding of the original problem in the ensemble case, and the best way to do this. By “best” way, this includes considerations such as: (i) requiring no complicated Hamiltonians beyond low-order products of total spin operators; (ii) the output of the quantum algorithm is not adversely affected by the generation of unstable quantum states such as Schrodinger cat states; (iii) the performance of the algorithm (as measured by e.g. success probability, fidelity, etc.) remains the same or acceptably high under realistic conditions. For these reasons, the mapping between qubit algorithms to EQC requires some analysis, and currently no general procedure exists to map between the two. Nevertheless, to date several algorithms have been shown to be mapped, including quantum teleportation [16, 17] and Deutsch’s algorithm [15].

In this paper we provide a full analysis of mapping the Deutsch-Jozsa algorithm to EQC. Our aim is to start with the qubit version of the algorithm, and convert this to an implementation using ensembles and ultimately a Hamiltonian involving only products of total spin operators. As mentioned above, as the EQC mapping involves mapping qubits onto ensembles, there are in fact many possible mappings which in principle accomplishes the task. Partly to this reason, we find two viable mappings, which are both presented in this paper. This paper is structured as follows. In Sec. II we give a review of the EQC framework, in the interest of this paper being self-contained. We then review the Deutsch-Jozsa algorithm for qubits in Sec. III A, which serves to introduce our notation. Due to the rather detailed nature of this paper, we then summarize in Sec. III B our final results for how to map the Deutsch-Jozsa algorithm onto EQC for readers who are not interested in the details of the proof. The remaining sections are devoted to the proof of how the EQC mapping works. One of the results that we will require is an explicit form of the oracle Hamiltonian for qubits, which is derived in Sec. IV. We show that some of these implementations are more favorable for the EQC than others. In the case that it is possible to choose exactly how the oracle is implemented, a mapping that is robust against decoherence for EQC is presented (Sec. VI). In the case that the oracle is strictly not choosable, and it must be mapped directly from the qubit case, we provide another mapping which works for all cases (Sec. V). We finally summarize our findings in Sec. VIII.

II. ENSEMBLE QUANTUM COMPUTATION

In this section we provide a brief summary of the essential aspects of EQC, for the benefit of this paper being self-contained. A more detailed description is given in Ref. [15].

In EQC, quantum information is stored on ensembles of two level systems. This can be either a large number of individual qubits such as an atomic ensemble, or a two-component Bose-Einstein condensate (BEC) [14, 15, 18, 19]. In this approach, the quantum information corresponding to a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ is stored as a spin coherent state. For an atomic ensemble, this is written

$$|\alpha, \beta\rangle \equiv \prod_{m=1}^N (\alpha|0\rangle_m + \beta|1\rangle_m) \quad (1)$$

where $|0\rangle_m$ and $|1\rangle_m$ are the logical states of the m th qubit in the ensemble. In the case of a BEC, the spin coherent state is

$$|\alpha, \beta\rangle \equiv \frac{1}{\sqrt{N!}} (\alpha a^\dagger + \beta b^\dagger)^N |0\rangle \quad (2)$$

where a, b are bosonic annihilation operators satisfying $[a, a^\dagger] = [b, b^\dagger] = 1$ corresponding to the two logical states that store the quantum information. In each case we assume a fixed number of particles N in the ensemble or BEC.

The states in (1) and (2) may be expanded in terms of Fock states with definite particle number. For the ensemble system we may define

$$|k\rangle = \frac{1}{\sqrt{\binom{N}{k}}} \sum_{\substack{x_1 x_2 \dots x_N \\ \{\sum_m x_m = N-k\}}} |x_1 x_2 \dots x_N\rangle, \quad (3)$$

where $x_m \in \{0, 1\}$ and the sum is restricted states with $N - k$ spins in the state $|1\rangle$ and k in the state $|0\rangle$. For the BEC case, the Fock states are

$$|k\rangle = \frac{1}{\sqrt{k!(N-k)!}} (a^\dagger)^k (b^\dagger)^{N-k} |0\rangle. \quad (4)$$

The spin coherent states (1) and (2) can be expanded using Fock states into

$$|\alpha, \beta\rangle = \sum_{k=0}^N \sqrt{\binom{N}{k}} \alpha^k \beta^{N-k} |k\rangle, \quad (5)$$

which is true for both the ensemble and BEC cases.

For manipulation of the state (1) and (2) we use the total spin operators

$$\begin{aligned} S^X &= \sum_{m=1}^N \sigma_m^X \\ S^Y &= \sum_{m=1}^N \sigma_m^Y \\ S^Z &= \sum_{m=1}^N \sigma_m^Z \end{aligned} \quad (6)$$

where $\sigma_m^{X,Y,Z}$ are the Pauli operators for each qubit in the ensemble, defined according to

$$\begin{aligned}\langle x' | \sigma^X | x \rangle &= \delta_{x,1-x'} \\ \langle x' | \sigma^Y | x \rangle &= i(-1)^x \delta_{x,1-x'} \\ \langle x' | \sigma^Z | x \rangle &= (-1)^x \delta_{x,x'}\end{aligned}\quad (7)$$

where $x \in \{0, 1\}$ and $\delta_{x,x'}$ is the Kronecker delta. For the BEC case, the total spin operators are Schwinger boson operators

$$\begin{aligned}S^X &= a^\dagger b + b^\dagger a \\ S^Y &= -ia^\dagger b + ib^\dagger a \\ S^Z &= a^\dagger a - b^\dagger b\end{aligned}\quad (8)$$

The Fock states are eigenstates of the S^Z operator, both for the ensemble and BEC cases we have

$$S^Z |k\rangle = (2k - N) |k\rangle. \quad (9)$$

The total spin operators obey the same commutation relations as Pauli operators

$$[S^i, S^j] = 2i\epsilon_{ijk} S^k \quad (10)$$

where ϵ_{ijk} is the Levi-Civita antisymmetric tensor. While (10) suggests an analogous structure to standard qubits, the total spin operators do not satisfy

$$\{S^i, S^j\} \neq 2\delta_{ij} \quad (11)$$

where δ_{ij} is the Kronecker delta. For qubits $N = 1$, the anticommutation relation is satisfied, which in many cases results in simplifications. For example, (11) implies that $(\sigma^{X,Y,Z})^2 = 1$, which is not true for the $N \geq 2$ case. For our calculations we will generally use the BEC formulation of the total spins (8) rather than the ensemble formulation (6) for the sake of mathematical simplicity. In fact these are equivalent as long as all physical operations and the initial conditions of the spins are symmetric under particle interchange. Thus either ensembles or BECs could be used experimentally.

The aim of EQC is then exploit the analogous structure of the spin coherent states to qubits to provide a framework for quantum computation. In the same way as qubits and CV approaches where many qubits and modes are used to store the quantum information, in a typical EQC algorithm one would use several ensembles, which are potentially entangled together. A typical entangling interaction between ensembles that is considered is a $H = S_1^Z S_2^Z$ interaction, as this can be implemented experimentally using several schemes [20–22]. Such an interaction produces in general a complex entangled state, exhibiting entanglement with a fractal structure [23, 24]. Nevertheless for particular gate times this has a simplified structure which may be used for quantum information tasks [16, 17].

One of the advantages of EQC is that quantum information is always stored in a highly duplicated way. This

allows for a more robust storage of quantum information as the loss or corruption of a few of the particles making up the ensemble impacts the total spin in a negligible way. This is in contrast to single particle storage methods where one qubit's worth of information is stored on one physical qubit. In this case if the particle is lost or an error occurs, all the quantum information is destroyed, which motivates quantum error correction. Another benefit is that experimentally manipulating ensembles is an easier task technically compared to single particles, with the additional benefit of an increased signal to noise in any measurement readout. Although not used in this paper, another benefit is that ensembles have the possibility of non-destructive readout, an operation which is fundamentally not possible with qubit based systems [25, 26].

Due to the larger Hilbert space available to the ensembles, given a quantum algorithm intended for qubits, in principle there are many ways to map it only the ensemble system. For example, one simple way would be to pick two states in the ensemble and use this as the logical states. However, such an approach would not be desirable as it would be experimentally challenging to target two particular states in the ensemble. By this we mean that exotic gates with complex Hamiltonians are required. It is also potentially susceptible to decoherence. For example, using an encoding of states such as $|0_L\rangle = |00\dots 0\rangle$ and $|1_L\rangle = |11\dots 1\rangle$ would correspond to using Schrodinger cat-like states, which are vulnerable to decoherence.

For these reasons we impose the following additional restrictions and assumptions when constructing a quantum algorithm in EQC:

- Only gates involving Hamiltonians with linear products of total spins $S^{X,Y,Z}$ are used.
- Measurements are made in a collective basis, e.g. S^Z .
- The performance of the algorithm should not degrade exponentially with particle number N under decoherence.
- The gate resource count for applying a gate to an ensemble is the same as for a qubit.

The first and second restrictions ensure that any algorithm constructed should be able to be implemented using reasonable means. As discussed in Ref. [22], collective operations are typically of the form of linear products of total spin operators $S^{X,Y,Z}$. The third restriction requires analysis of the quantum algorithm under the presence of decoherence. For example, if the algorithm generates Schrodinger cat states and stores quantum information that affects the quantum algorithm, this could adversely affect the performance.

The last assumption is important from the point of view of whether a quantum algorithm has been mapped

correctly with a quantum speedup. Since an ensemble involves N individual qubits, a question arises of whether we count resources on a per qubit or per ensemble basis. In our method, we take the latter approach for the reason that only collective operations are performed on the ensembles. When applying a collective operation to ensembles, we assume that it is no more difficult (i.e. experimentally time consuming) to perform the operation on the ensemble as compared to the qubit. For example, in the case of the optical manipulation of Ref. [22], a Raman laser pulse performs an S^X rotation of the ensemble. In this case, the time required in order to rotate one qubit compared to N qubits is the same, as the same laser pulse illuminates all atoms simultaneously. Counted in this way, we consider a single gate to operate on all the qubits within an ensemble in parallel, such that gate resource counts are the same for an ensemble and a single qubit.

III. DEUTSCH-JOSZA ALGORITHM

A. Qubit implementation

In this section we review the Deutsch-Jozsa algorithm for qubits, which will serve to introduce our notation and highlight several aspects of the algorithm which will be useful later. In particular, we derive explicit expressions for the Hamiltonian of the oracle, which plays a central role in the algorithm.

Consider a function $f(x)$ which takes an integer input $x \in [0, 2^M - 1]$ and outputs a binary result $f \in [0, 1]$ (see Fig. 1a). The types of functions that are allowable to two types. The first type, called “constant”, has an output which is constant for all x . There are only two types of constant functions, $f = 0$ and $f = 1$. The second type, called “balanced”, has exactly half its output being 0 and the other half being 1. There are $\binom{2^M}{2^{M-1}}$ such balanced functions. Now consider that we are given a device, the “oracle”, that implements the function $f(x)$ according to the above restrictions. The aim of the Deutsch-Jozsa algorithm is to discriminate a given function $f(x)$ between the balanced and constant cases, with as few calls to the oracle as possible. Classically, to make this classification with certainty, it is necessary to call the oracle more than half the number of input values, i.e. $2^{M-1} + 1$ times.

Quantum mechanically, it is possible to speed this up exponentially. The oracle is implemented such that it follows a relation

$$U_f|y\rangle|x\rangle = |y \oplus f(x)\rangle|x\rangle \quad (12)$$

where $y \in [0, 1]$ and \oplus is the logical XOR gate. The x -register consists of M qubits in a binary representation, as shown in Fig. 1b. Assuming that the oracle can take a superposition of input states, then the quantum circuit Fig. 1b achieves the objective with only one call of the oracle [27]. For the case that $f(x)$ is constant, the measurement yields a result with all the x -register qubits in

the state $|0\rangle$. For $f(x)$ balanced, the measurement yields a result with at least one of the x -register qubits in the state $|1\rangle$. We summarize the effect of the circuit Fig. 1b as

$$|1\rangle|x=0\rangle \rightarrow \begin{cases} \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) |x=0\rangle & f(x) \in \text{constant} \\ \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) |x>0\rangle & f(x) \in \text{balanced} \end{cases} \quad (13)$$

The output of the x -register unambiguously discriminates between the constant and balanced cases, which achieves the objective of the Deutsch-Jozsa algorithm.

In this paper, we distinguish between two modes of oracle operation: “classical” and “quantum”. When the oracle has no superposition states as its input, such as in (12), we call the oracle to be operating in “classical” mode. When the inputs are in a superposition state, such as that shown in Fig. 1b, we say that the oracle is operating in “quantum” mode. There is no difference to the operation of the oracle itself in either case – the only difference is what states are input to the oracle.

B. EQC implementation

Here we present a summary of the Deutsch-Jozsa algorithm in the EQC framework, for the benefit of readers who are not interested in following the details of the proof in the following sections. We show two methods of mapping the Deutsch-Jozsa algorithm, which are distinct in the way the oracle and quantum information are defined. In both cases, the basic procedure is to follow the quantum circuit of Fig. 1(b). The definition of each of the components in the circuit are however different, and are defined in Table I.

We point out that as seen in Table I, all the gates performed are collective operations, involving a Hamiltonian of only linear powers of total spin operators $S^{X,Y,Z}$. The Hadamard gate for EQC reads as

$$\begin{aligned} a &\rightarrow \frac{a-b}{\sqrt{2}} \\ b &\rightarrow \frac{a+b}{\sqrt{2}}, \end{aligned} \quad (14)$$

which corresponds to applying a Hamiltonian S^Y for a time $\pi/4$. Similarly, the measurement is in the collective basis of the eigenstates of the S^Z operators. This is one of the requirements of EQC, such that it can be realistically implemented experimentally.

IV. THE DEUTSCH-JOSZA ORACLE

Typically in the discussion of the Deutsch-Jozsa algorithm the specific implementation of the oracle is left unspecified, as this is the object which we are trying to gain

Component in Deutsch-Jozsa algorithm	Method 1	Method 2
$ 0\rangle_L$	$ 0, 1\rangle$	$ 0, 1\rangle$
$ 1\rangle_L$	Fock state $ k_0\rangle$, with $k_0 \in \text{odd}$	$ 1, 0\rangle$
Hadamard Hamiltonian	S^Y	S^Y
Oracle Hamiltonian mapping	$\sigma^Z \rightarrow S^Z + N + 1$	$\sigma^Z \rightarrow S^Z / N$
Measurement	S^Z basis	S^Z basis
Constant outcome	$\forall n : 0, 1\rangle_n$	$\forall n : 0, 1\rangle_n$
Balanced outcome	Any state orthogonal to $\forall n : 0, 1\rangle_n$	Any state orthogonal to $\forall n : 0, 1\rangle_n$

TABLE I. Summary of mapping of the Deutsch-Jozsa algorithm for ensemble quantum computation. In both Methods 1 and 2, the quantum circuit of Fig. 1(b) is followed, with the definitions as given in the table. The outcome of the measurement for balanced oracle cases are the converse of the constant cases.

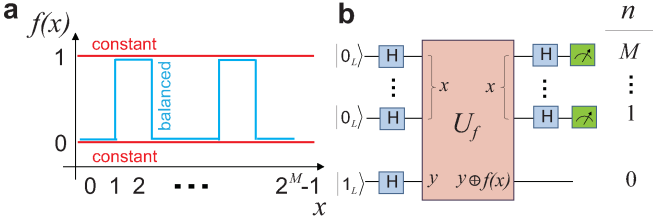


FIG. 1. The Deutsch-Jozsa algorithm. (a) The function $f(x)$ which determines the oracle. (b) The quantum circuit for the Deutsch-Jozsa algorithm. The gates marked by H are Hadamard gates, U_f is the oracle, and the meter symbols denote a measurement in S^Z -basis. The labeling of the qubits/ensembles for $n \in [0, M]$ is shown.

information about. There are in fact an infinite number of ways that the relation (12) can be performed. However, for a mapping to EQC it is an important question to understand whether the oracle itself can be implemented using ensembles, as now the input of the circuit Fig. 1b are each ensembles instead of qubits. What is the meaning of (12) in an EQC implementation? To this end, we discuss specifically what qubit Hamiltonian is required for a given $f(x)$ to realize the oracle.

A. Oracle Hamiltonian

Let us start by first writing an explicit form of the unitary of the oracle according to the definition (12). The unitary corresponding to the oracle is

$$U_f = \sum_{x=0}^{2^M-1} [(1 - f(x))I_0 + f(x)\sigma_0^X] |x\rangle\langle x| \quad (15)$$

Looking at each term in the summation, for any x with $f(x) = 0$, the unitary reduces to $U_f = |x\rangle\langle x|$, which leaves the state of y unchanged. For any x with $f(x) = 1$, the unitary is $U_f = \sigma_0^X |x\rangle\langle x|$, which flips the state of y . We see that for the case of constant $f(x)$, the results of (17) and (19) are recovered. To make this relation more

explicit, let us rewrite (15) according to

$$U_f = \sum_{x \notin \mathcal{F}} |x\rangle\langle x| + \sigma_0^X \sum_{x \in \mathcal{F}} |x\rangle\langle x| \quad (16)$$

where \mathcal{F} is the set of all x that satisfy $f(x) = 1$.

Now let us explicitly write the Hamiltonians which give rise to (16) first for the constant cases. In the case that $f = 0$, this leaves both $|x\rangle$ and $|y\rangle$ unchanged hence this may be implemented by

$$U_{f=0} = e^{-iH_{f=0}t} = I \quad (17)$$

where I is the identity operator on the whole system. Assuming throughout for concreteness that the Hamiltonian is always evolved for a time $t = 1$, a Hamiltonian that implements this is

$$H_{f=0} = 2\pi j \quad (18)$$

where j is an arbitrary integer.

For the function $f = 1$, this results in always flipping the y -qubit, which can be implemented by

$$U_{f=1} = e^{-iH_{f=1}t} = \sigma_0^X. \quad (19)$$

A Hamiltonian that satisfies this is

$$H_{f=1} = \pi(2j + 1) \left(\frac{\sigma_0^X - I_0}{2} \right) \quad (20)$$

again for a time $t = 1$ and j is an arbitrary integer. Here σ_0^X, I_0 denotes the Pauli and identity operator on the $n = 0$ qubit, following the labels as specified in Fig. 1b. The factor of $2j + 1$ reflects the fact that any odd integer may multiply the Hamiltonian with the same effect. In this case this degree of freedom does not play an important role, however we will see that this gives an important degree of freedom when constructing balanced Hamiltonians.

Now let us turn to the balanced cases. Before constructing the Hamiltonian for (16), it is instructive to calculate the Hamiltonian for an oracle where only one of the x 's satisfies $f(x) = 1$, that is

$$f_x(x') = \begin{cases} 1 & x' = x \\ 0 & x' \neq x \end{cases} \quad (21)$$

In this case the oracle gives

$$U_x = \sum_{x' \neq x} |x'\rangle\langle x'| + \sigma_0^X |x\rangle\langle x|. \quad (22)$$

Similarly to (20), we can write

$$H_x = \pi(2j_x + 1) \left(\frac{\sigma_0^X - I_0}{2} \right) |x\rangle\langle x|, \quad (23)$$

which can be verified to satisfy $U_x = e^{-iH_x t}$ for a time evolution $t = 1$, using $e^{iA|x\rangle\langle x|} = I + (e^{iA} - I)|x\rangle\langle x|$ for an arbitrary operator A . Here j_x is an integer that can be independently chosen for each x . Rewriting the projection operator in terms of Pauli matrices, this is

$$\begin{aligned} H_x &= \pi(2j_x + 1) \left(\frac{\sigma_0^X - I_0}{2} \right) \prod_{n=1}^M \frac{1}{2} (1 + (-1)^{x_n} \sigma_n^Z) \\ &= \pi(2j_x + 1) \left(\frac{\sigma_0^X - I_0}{2} \right) \frac{1}{2^M} \left[1 + \sum_n (-1)^{x_n} \sigma_n^Z \right. \\ &\quad \left. + \sum_n \sum_{n' \neq n} (-1)^{x_n + x_{n'}} \sigma_n^Z \sigma_{n'}^Z + \cdots + \prod_{n=1}^M (-1)^{x_n} \sigma_n^Z \right] \\ &= \pi(2j_x + 1) \left(\frac{\sigma_0^X - I_0}{2} \right) \sum_{z=0}^{2^M-1} \frac{(-1)^{z \cdot x}}{2^M} \prod_{n=1}^M (\sigma_n^Z)^{z_n}, \end{aligned} \quad (24)$$

where in the second line we have expanded the product to a sum of various products of Pauli matrices. There are 2^M terms in the expansion, and each of the terms in the expansion is labeled by $z \in [0, 2^M - 1]$. The x_n, z_n are binary representations of x and z , where n is the bit label, and $x \cdot z = \sum_n x_n z_n$.

Once we have the Hamiltonian that gives the unitary (22) for one of the x 's, the Deutsch-Jozsa oracle (16) can be constructed by multiplying together all the cases that satisfy $f(x) = 1$. That is,

$$U_f = \prod_{x \in \mathcal{F}} U_x. \quad (25)$$

As all the different H_x for all x commute, the total Hamiltonian is simply the sum of those satisfying $x \in \mathcal{F}$:

$$\begin{aligned} H_f &= \sum_{x \in \mathcal{F}} H_x \\ &= \pi \left(\frac{\sigma_0^X - I_0}{2} \right) \sum_{x \in \mathcal{F}} (2j_x + 1) |x\rangle\langle x| \\ &= \pi \left(\frac{\sigma_0^X - I_0}{2} \right) \sum_{x \in \mathcal{F}} (2j_x + 1) \prod_{n=1}^M \frac{1}{2} (1 + (-1)^{x_n} \sigma_n^Z) \end{aligned} \quad (26)$$

Expanding the product, the Hamiltonian can then be written explicitly as

$$H_f = \pi \left(\frac{\sigma_0^X - I_0}{2} \right) \sum_{z=0}^{2^M-1} \alpha_z \prod_{n=1}^M (\sigma_n^Z)^{z_n}. \quad (27)$$

where

$$\alpha_z = \frac{1}{2^M} \sum_{x \in \mathcal{F}} (2j_x + 1) (-1)^{z \cdot x}. \quad (28)$$

It is convenient for later to define the coefficients of the expanded version of the Hamiltonian

$$\begin{aligned} H_f &= \pi \left(\frac{\sigma_0^X - I_0}{2} \right) \left[\alpha_0 + \sum_n \alpha_n \sigma_n^Z + \sum_n \sum_{n' \neq n} \alpha_{nn'} \sigma_n^Z \sigma_{n'}^Z \right. \\ &\quad \left. + \cdots + \alpha_{12 \dots M} \prod_{n=1}^M \sigma_n^Z \right] \end{aligned} \quad (29)$$

where the coefficients are

$$\begin{aligned} \alpha_0 &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (2j_x + 1), \\ \alpha_n &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (2j_x + 1) (-1)^{x_n}, \\ \alpha_{nn'} &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (2j_x + 1) (-1)^{x_n + x_{n'}}, \\ &\vdots \\ \alpha_{12 \dots M} &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (2j_x + 1) (-1)^{\sum_n x_n}. \end{aligned} \quad (30)$$

Here the j_x are integers that may be chosen freely. In fact it is possible to generalize (28) further if necessary, by for example adding an even integer to α_z . This shows that the Hamiltonian that implements the oracle has a large amount of freedom associated with it. For our purposes the above Hamiltonian is general enough and will serve as representing a simple set of practical implementations of the oracle.

B. Example and Implications

To illustrate the difference in choice of Hamiltonians, let us consider a simple example. Let us consider the case $M = 2$, and a balanced oracle function such that $f(x) = 1$ for $\{|00\rangle, |11\rangle\}$ and $f(x) = 0$ for $\{|01\rangle, |10\rangle\}$. Choosing $j_x = 0$, we have

$$\begin{aligned} \alpha_0 &= \frac{1}{2} \\ \alpha_n &= 0 \\ \alpha_{12} &= \frac{1}{2}. \end{aligned} \quad (31)$$

The oracle Hamiltonian is thus

$$H_f = \frac{\pi}{4} (\sigma_0^X - 1) (1 + \sigma_1^Z \sigma_2^Z). \quad (32)$$

First consider operating in “classical” mode where the inputs of the x -register is one of the logical states $|x\rangle$

with no superposition. For states with $x \in \mathcal{F}$, we have $\sigma_1^Z \sigma_2^Z |x\rangle = |x\rangle$. Then

$$\begin{aligned} e^{-iH_f t} |y\rangle |x\rangle &= e^{-i\pi(\sigma_0^X - 1)/2} |y\rangle |x\rangle \\ &= |\bar{y}\rangle |x\rangle \end{aligned} \quad (33)$$

where $\bar{y} = 1 - y$. The Hamiltonian thus flips the y -qubit on this cases. For $x \notin \mathcal{F}$, $\sigma_1^Z \sigma_2^Z |x\rangle = -|x\rangle$ and

$$e^{-iH_f t} |y\rangle |x\rangle = |y\rangle |x\rangle \quad (34)$$

which leaves the y -qubit unaffected. Operating in “quantum” mode (i.e. the circuit of Fig. 1(b)), we have

$$\begin{aligned} e^{-iH_f t} |-\rangle |+\rangle |+\rangle &= e^{i\pi(1+\sigma_1^Z \sigma_2^Z)/2} |-\rangle |+\rangle |+\rangle \\ &= \sigma_1^Z \sigma_2^Z |-\rangle |+\rangle |+\rangle \\ &= |-\rangle |-\rangle |-\rangle \end{aligned} \quad (35)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. In the above we have used the identity $\exp(i\theta \prod_n \sigma_n^Z) = \cos \theta + i \sin \theta \prod_n \sigma_n^Z$. The Hadamard gate then rotates the above state to $|-\rangle |1\rangle |1\rangle$, which is then measured showing that the oracle is balanced.

A difference choice of the free parameters however can produce the same result. Now let us choose for the same function $j_{x=|00\rangle} = 0$ and $j_{x=|11\rangle} = -1$. This time we obtain

$$\begin{aligned} \alpha_0 &= 0 \\ \alpha_n &= \frac{1}{2} \\ \alpha_{12} &= 0, \end{aligned} \quad (36)$$

which gives a Hamiltonian

$$H'_f = \frac{\pi}{4} (\sigma_0^X - 1) (\sigma_1^Z + \sigma_2^Z). \quad (37)$$

In “classical” mode, for $x \in \mathcal{F}$, the states evolve as

$$\begin{aligned} e^{-iH'_f t} |y\rangle |x\rangle &= e^{\pm i\pi(\sigma_0^X - 1)/2} |y\rangle |x\rangle \\ &= |\bar{y}\rangle |x\rangle \end{aligned} \quad (38)$$

which again flips the y -qubit. For cases where $x \notin \mathcal{F}$, the state remains unchanged. In “quantum” mode, we have

$$\begin{aligned} e^{-iH'_f t} |-\rangle |+\rangle |+\rangle &= e^{i\pi(\sigma_1^Z + \sigma_2^Z)/2} |-\rangle |+\rangle |+\rangle \\ &= \sigma_1^Z \sigma_2^Z |-\rangle |+\rangle |+\rangle \\ &= |-\rangle |-\rangle |-\rangle \end{aligned} \quad (39)$$

We thus see that the two Hamiltonian implementations lead to the same oracle.

It may appear curious that the Hamiltonians (32) and (37) lead to the same result, despite the fact that (32) is an entangling Hamiltonian, but (37) clearly never produces entanglement. The reason for this are the special coefficients which for this case never result in any entanglement being generated between the qubits. Evolving

a Hamiltonian $H = \pi \sigma_1^Z \sigma_2^Z / 2$ applied to a state $|+\rangle |+\rangle$ initially creates entanglement, but at the time $t = 1$ disentangles the qubits again.

Based on the above result, one may speculate that perhaps it is possible to always choose an oracle Hamiltonian without any entangling terms. This is in fact false, and is a special case for $M \leq 2$. To see this, consider the $M = 3$ case and $f(x) = 1$ for $\{|000\rangle, |001\rangle, |010\rangle, |100\rangle\}$ and $f(x) = 0$ otherwise. Operating in “quantum” mode, then from (16) it can be seen that the oracle flips the sign of states with $x \in \mathcal{F}$. The oracle then performs the operation

$$\begin{aligned} |+\rangle |+\rangle |+\rangle &\rightarrow \frac{1}{2} (|1\rangle |1\rangle - |0\rangle |0\rangle) |+\rangle \\ &\quad - \frac{1}{2} (|0\rangle |1\rangle + |1\rangle |0\rangle) |-\rangle \end{aligned} \quad (40)$$

which is obviously an entangled state.

V. EQC MAPPING METHOD 1: EXACT APPROACH

In this section we present the first of two methods of mapping the Deutsch-Jozsa algorithm to the EQC framework. In this method, it is possible to exactly map the qubit version of the circuit to ensembles. This is possible for any choice of oracle, i.e. any of the freely choosable parameters in the oracle Hamiltonian. Furthermore, the success probability is exactly 1, as in the qubit case. The mapping however requires the preparation of Fock states, and is more susceptible to decoherence. We later present an alternative approach that overcomes some of these issues at the expense of loss of generality of the oracle.

A. Encoding

Before introducing the quantum algorithm for Deutsch-Jozsa in EQC, we must settle on the encoding for the oracle. In EQC, qubits are replaced by ensembles, hence there will be one ensemble which encodes the y -qubit, and M ensembles encoding the x -register.

In this section we choose an encoding

$$\begin{aligned} |0_L\rangle &\equiv |k \in \text{even}\rangle \\ |1_L\rangle &\equiv |k \in \text{odd}\rangle \end{aligned} \quad (41)$$

where $k \in [0, N]$ and the states on the right hand side are the Fock states as defined in (3) and (4). The above definition clearly has a redundancy as more than one state can encode the logical states. This means that any one – or superposition – of the states that satisfy the above qualifies to be a logical state. For example, any superposition of even k Fock states would be interpreted as a logical $|0_L\rangle$ state.

The above encoding is used for each of the qubits involved in the x -register and the y -qubit. For a given Fock

state in the x -register

$$|x\rangle = |k_1 k_2 \dots k_M\rangle, \quad (42)$$

we may obtain the logical version of this by the relation

$$(x_n)_L = k_n \mod 2. \quad (43)$$

Under the above encoding, we may obtain a generalized method for mapping the qubit Hamiltonians into ensemble based Hamiltonians for $N > 1$. Specifically we perform the mapping

$$\sigma^Z \rightarrow S^Z + N + 1. \quad (44)$$

To understand the origin of this mapping, consider a simple example of mapping the projection operators to the ensemble spins. Writing the right hand side in terms of Fock states, we have

$$|0\rangle\langle 0| = \frac{1}{2}(1 + \sigma^Z) \rightarrow \sum_{k=0}^N (k+1) |k\rangle\langle k|. \quad (45)$$

Now consider that this is the Hamiltonian, and it is evolved for a particular time $t = \pi$. For qubits we can evaluate

$$e^{-i\pi|0\rangle\langle 0|} = |1\rangle\langle 1| - |0\rangle\langle 0|. \quad (46)$$

For the ensemble case, we have

$$e^{-i\pi \sum_{k=0}^N (k+1) |k\rangle\langle k|} = \sum_{k \in \text{odd}} |k\rangle\langle k| - \sum_{k \in \text{even}} |k\rangle\langle k|. \quad (47)$$

We thus see that under the encoding (41) the effect of the mapping is the same, that it adds a negative sign for the logical 0 states, and keeps the original phase for the logical 1 states. A similar result is obtained for the logical 1 projector using

$$|1\rangle\langle 1| = \frac{1}{2}(1 - \sigma^Z) \rightarrow \sum_{k=0}^N (-k) |k\rangle\langle k|. \quad (48)$$

B. Oracle definition: “classical” mode operation

In order that the Deutsch-Jozsa algorithm be executed in the EQC framework, we must ensure that the oracle itself can be constructed using the constraints as discussed in Sec. II. Specifically, we demand that the Hamiltonian is made of terms that are at most linear in total spin operators $S_n^{X,Y,Z}$. Let us verify that the mapping (44) for oracle Hamiltonian as given by (26) indeed gives the desired output, working in “classical” mode. Substituting, we obtain

$$\begin{aligned} H_f &= \frac{\pi(S_0^X + N_0)}{2} \sum_{x' \in \mathcal{F}} (2j_{x'} + 1) \prod_{n=1}^M \left(\frac{S_n^Z + N_n}{2} + \bar{x}'_n \right) \\ &= \frac{\pi(S_0^X + N_0)}{2} \sum_{x' \in \mathcal{F}} (2j_{x'} + 1) \\ &\quad \otimes \sum_{k_1 \dots k_M} (k_1 + \bar{x}'_1) \dots (k_M + \bar{x}'_M) |k_1 \dots k_M\rangle \langle k_1 \dots k_M| \end{aligned} \quad (49)$$

where $\bar{x}'_n = 1 - x'_n$ and in the first line we have taken advantage of the fact that the $j_{x'}$ can be freely chosen to absorb an appropriate factor of ± 1 for each term in the sum.

With the oracle operating in “classical” mode, the x -register is prepared in a particular state (42) which represents a particular logical state according to (43). The y -register can be prepared in an arbitrary state in general, lets us choose $|0, 1\rangle\rangle$ which will illustrate the effect. Evolving (49) for $t = 1$ we obtain

$$\begin{aligned} e^{-iH_f t} |0, 1\rangle\rangle |k_1 \dots k_M\rangle &= \\ \exp \left[-i \frac{\pi}{2} (S_0^X + N_0) \sum_{x' \in \mathcal{F}} (2j_{x'} + 1) \prod_{n=1}^M (k_n + \bar{x}'_n) \right] \\ &\times |0, 1\rangle\rangle |k_1 \dots k_M\rangle \end{aligned} \quad (50)$$

Let us first examine the parity of product for a particular term x' under the summation. Due to the property of multiplication of odd and even integers

$$\begin{aligned} \text{even} \times \text{even} &= \text{even} \\ \text{even} \times \text{odd} &= \text{even} \\ \text{odd} \times \text{odd} &= \text{odd}, \end{aligned} \quad (51)$$

this means that the only time that the product can evaluate to an odd integer is when

$$x'_n = k_n \mod 2. \quad (52)$$

That is, the product is odd only when the logical state of the $|x\rangle = |k_1 \dots k_M\rangle$ state matches the specified x' . In all other cases the product evaluates to an even integer.

Now consider the summation over x' . There are two possible cases, either the chosen logical $|x\rangle$ state lies in \mathcal{F} , or not. For $x \notin \mathcal{F}$, all the terms in the sum are even, and due to the property of addition of integers

$$\begin{aligned} \text{even} + \text{even} &= \text{even} \\ \text{even} + \text{odd} &= \text{odd} \\ \text{odd} + \text{odd} &= \text{even}, \end{aligned} \quad (53)$$

the sum will yield an even integer. For $x \in \mathcal{F}$, then there will be exactly one term in the sum that is an odd number when $x' = x$, and all the remaining even. Thus the sum yields an odd number for this case. In summary, the evolved state reduces to

$$\exp \left[-i \frac{\pi}{2} (S_0^X + N_0) P_x \right] |0, 1\rangle\rangle |k_1 \dots k_M\rangle \quad (54)$$

where

$$P_x = \begin{cases} \text{odd} & \text{if } x \in \mathcal{F} \\ \text{even} & \text{if } x \notin \mathcal{F} \end{cases}. \quad (55)$$

For $P_x = 1$, the y -ensemble is rotated by an angle π on the Bloch sphere, flipping its orientation. Thus for

$x \in \mathcal{F}$, the y -ensemble is rotated by an odd number of flips, and for $x \notin \mathcal{F}$, an even number of flips:

$$e^{-iH_f t} |0, 1\rangle |x\rangle = \begin{cases} |1, 0\rangle |x\rangle & x \in \mathcal{F} \\ |0, 1\rangle |x\rangle & x \notin \mathcal{F} \end{cases}, \quad (56)$$

up to an global phase factor. We thus see that oracle has the effect of rotating the y -ensemble depending on whether the x -register state is contained in \mathcal{F} , which is the equivalent effect of the qubit oracle.

C. “Quantum” mode operation

We now evaluate the operation of the oracle within the quantum circuit as shown in Fig. 1(b). According to the encoding (41), the x -register must be prepared in an even parity state, while the y -ensemble must be prepared in an odd parity state. For simplicity we choose

$$\begin{aligned} |x\rangle &= \prod_{n=1}^M |k_n = 0\rangle = \prod_{n=1}^M |0, 1\rangle_n \\ |y\rangle &= |k_0\rangle \end{aligned} \quad (57)$$

where $k_0 \in \text{odd}$. After the Hadamard gates, this becomes

$$\begin{aligned} |x\rangle &= \prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n \\ |y\rangle &= |k_0\rangle_x, \end{aligned} \quad (58)$$

where $|k_0\rangle_x$ is a Fock state in the S^X basis. The x -register is now in a superposition involving all states $|k_1 \dots k_M\rangle$.

Let us see what the effect of the Hamiltonian (49) is for a general superposition state on the x -register. Evolving for a time $t = 1$, we have

$$\begin{aligned} e^{-iH_f t} \sum_{k_1 \dots k_M} \psi_{k_1 \dots k_M} |k_0\rangle_x |k_1 \dots k_M\rangle = \\ \sum_{k_1 \dots k_M} \psi_{k_1 \dots k_M} \exp \left[-i\pi k_0 \sum_{x' \in \mathcal{F}} (2j_{x'} + 1) \prod_{n=1}^M (k_n + \bar{x}'_n) \right] \\ \times |k_0\rangle_x |k_1 \dots k_M\rangle. \end{aligned} \quad (59)$$

For the specific initial condition that we consider, the coefficient is

$$\psi_{k_1 \dots k_M} = \prod_{n=1}^M \sqrt{\frac{1}{2^{N_n}}} \binom{N_n}{k_n}. \quad (60)$$

The sum in the exponent is the same quantity as that examined in the previous section, and using the property of multiplication of odd and even integers we have

$$\begin{aligned} e^{-iH_f t} \sum_{k_1 \dots k_M} \psi_{k_1 \dots k_M} |k_0\rangle_x |k_1 \dots k_M\rangle \\ = \sum_{k_1 \dots k_M} \psi_{k_1 \dots k_M} |k_0\rangle_x (-1)^{P_x} |k_1 \dots k_M\rangle. \end{aligned} \quad (61)$$

We see that the effect of the Hamiltonian in “quantum” mode is to change the sign of all the terms that satisfy $x \in \mathcal{F}$ under the encoding (43).

We must now apply another Hadamard gate to the x -register, which is most easily done in the spin coherent state representation. Define the even Schrodinger cat states as

$$\begin{aligned} |+\rangle &\equiv \frac{1}{\sqrt{2^N}} \sum_{k \in \text{even}} \sqrt{\binom{N}{k}} |k\rangle \\ &= \frac{1}{\sqrt{2}} \left(\left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle + \left| \frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle \right) \end{aligned} \quad (62)$$

while the odd Schrödinger cat states are

$$\begin{aligned} |-\rangle &\equiv \frac{1}{\sqrt{2^N}} \sum_{k \in \text{odd}} \sqrt{\binom{N}{k}} |k\rangle \\ &= \frac{1}{\sqrt{2}} \left(\left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle - \left| \frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle \right). \end{aligned} \quad (63)$$

The above was for one ensemble. The state for a particular logical x -state may then be specified according to

$$\prod_{n=1}^M |(-1)^{x_n}\rangle \quad (64)$$

which is a superposition of states of the same parity as given in (42). Using this notation, the state (61) for the coefficients (60) can be written

$$\begin{aligned} e^{-iH_f t} |k_0\rangle_x \prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n \\ = |k_0\rangle_x \left(\prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n \right. \\ \left. - 2 \sum_{x \in \mathcal{F}} \prod_{n=1}^M |(-1)^{x_n}\rangle \langle (-1)^{x_n} | \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \rangle_n \right) \end{aligned} \quad (65)$$

where we have projected the parts with the specified parity in (64) and subtracted twice this in order to change the sign of these terms. Since

$$\langle \langle \pm | \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \rangle \rangle = \frac{1}{\sqrt{2}} \quad (66)$$

we then obtain

$$\begin{aligned} e^{-iH_f t} |k_0\rangle_x \prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n = |k_0\rangle_x \left[\prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n \right. \\ \left. - \frac{2}{2^M} \sum_{x \in \mathcal{F}} \prod_{n=1}^M \left(\left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n + (-1)^{x_n} \left| \frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n \right) \right]. \end{aligned} \quad (67)$$

Noting that there are $2^M/2$ terms in the x summation, and the coefficient of $\prod_{n=1}^M |\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\rangle_n$ exactly cancels. The set of Hadamard gates on the x -register after the oracle operation finally gives the state

$$\begin{aligned} & \prod_{n=1}^M |0, 1\rangle_n - \frac{2}{2^M} \sum_{x \in \mathcal{F}} \prod_{n=1}^M (|0, 1\rangle_n + (-1)^{x_n} |1, 0\rangle_n) \\ &= -\frac{2}{2^M} \sum_{z=1}^{2^M-1} \sum_{x \in \mathcal{F}} (-1)^{z \cdot x} \prod_{n=1}^M |z_n, 1 - z_n\rangle, \end{aligned} \quad (68)$$

where z is an expansion index ordinarily running from $z \in [0, 2^M - 1]$, in the same way as (24). This state has exactly zero overlap with the state $\prod_{n=1}^M |0, 1\rangle_n$, as the $z = 0$ term exactly cancels, and due to $|0, 1\rangle$ and $|1, 0\rangle$ being orthogonal. For a “constant” oracle, the overlap with $\prod_{n=1}^M |0, 1\rangle_n$ is on the other hand 1. Thus we have perfect distinguishability between the two cases and the same result for qubits has been recovered for the ensemble based method.

The above result is the desired result in the sense that a general mapping has been obtained for an arbitrary oracle and works with (in the ideal case) probability 1. There are some aspects which may be concerning from a practical perspective. The first is that the odd/even encoding (41) requires that one be able to prepare Fock states with a particle number resolution of 1, which can be very difficult in practice. While this may seem to make the scheme presented here unrealistic, in fact the prepared Fock states never possess any dynamics and remain static throughout both the “classical” and “quantum” circuits. For example, in the “classical” circuit the x -register is an eigenstate of the Hamiltonian and is unaffected by the oracle. In “quantum” operation the y -ensemble is an eigenstate, and again remains unaffected. Thus it would be possible to treat both these initializations classically by replacing these terms in the Hamiltonian by the desired constant.

Another concerning aspect is that the final state involves Schrodinger cat states (62) and (63). Such states are notoriously unstable and in a realistic setting are likely to decohere very quickly. As explained in Sec. II, in an ideal mapping from qubits to EQC, we would like to map the problem so that the decoherence is no worse than for the original qubit problem. This is however at odds with the very concept of an oracle, as it is considered to be a “black box” and its inner workings left unspecified. It is therefore always possible to create pathological implementations of the oracle which are highly susceptible to decoherence – for instance one that creates a Schrodinger cat, reverses the operation to revert to the original state, then perform the oracle. Thus the emergence of Schrodinger cat states in the current encoding is the price to be paid for allowing a completely general implementation of an oracle. As we will see in the next section, some choices of the oracle implementation are better than others, when it is assumed that decoher-

ence is present. Thus by preferring certain oracle implementation choices, it becomes possible to implement the Deutsch-Jozsa algorithm in a more robust way.

VI. EQC MAPPING METHOD 2: CHOOSABLE ORACLE

In the previous section, we presented a general mapping from the qubit version of the Deutsch-Jozsa algorithm to its EQC implementation. While the approach has the advantage that it is completely general, it has the drawback that some undesirable decoherence-prone Schrodinger cat states are generated, and the preparation of Fock states are required. The reason that such undesirable states are involved is to accommodate a completely general oracle, which introduces Schrodinger cat states. If this requirement is relaxed, then it is possible to use other encodings, which avoids some of these difficulties.

This may appear to be introducing additional assumptions into the Deutsch-Jozsa algorithm. Nevertheless, we note that the speedup compared to the classical case is still exponential. Consider the scenario that the particular oracle implementations for each $f(x)$ is agreed upon initially and chosen in a way that it satisfies – in a suitable encoding – the “classical” mode definition (12). One of the oracles is then chosen without knowing which of the $\binom{2^M}{2^{M-1}} + 2$ types of $f(x)$ it implements. The task is then to find whether the $f(x)$ is constant or balanced, in the same way as the qubit Deutsch-Jozsa algorithm. We shall see that this task can be achieved with a probability exponentially close to 1, with only one call of the oracle. Thus the main aspect of the Deutsch-Jozsa algorithm is preserved with a quantum mechanical speedup over the classical case.

A. Encoding

The first step is again to define what the logical states that encode the inputs and outputs of the oracle are. In this approach, we define logical states with an analogous state on the Bloch sphere for the ensembles as for qubits. Hence the logical states for $y \in \{0, 1\}$ have a correspondence

$$|y\rangle \leftrightarrow |y\rangle \equiv |y, 1 - y\rangle \quad (69)$$

for the y -qubit, which is now a y -ensemble, and for the x -register we have

$$\begin{aligned} |x\rangle &\equiv |x_1\rangle |x_2\rangle \dots |x_M\rangle \\ &\updownarrow \\ |x\rangle &\equiv |x_1, 1 - x_1\rangle |x_2, 1 - x_2\rangle \dots |x_M, 1 - x_M\rangle, \end{aligned} \quad (70)$$

where we assume $x_n \in \{0, 1\}$.

For this encoding, the Pauli operators are mapped according to

$$\sigma^Z \rightarrow \frac{S^Z}{N}. \quad (71)$$

The normalization with N means that when the mapped operator acts on a state

$$\frac{S^Z}{N} |k\rangle = \left(\frac{2k}{N} - 1 \right) |k\rangle \quad (72)$$

where $k \in [0, N]$, so that for the extremal states $|k = 0\rangle = |0, 1\rangle$ and $|k = N\rangle = |1, 0\rangle$,

$$\frac{S_n^Z}{N_n} |x\rangle = (\pm 1)^{x_n} |x\rangle, \quad (73)$$

which is identical to the qubit case.

B. Oracle definition: “classical” mode operation

We first write the effect of the oracle working in “classical” mode, under the encodings (69) and (70). From the qubit definition (12), writing the ensembles explicitly a valid oracle for EQC must satisfy

$$\begin{aligned} U_f |y\rangle |x\rangle &= U_f |y, 1 - y\rangle \prod_{n=1}^M |x_n, 1 - x_n\rangle \\ &= |y \oplus f(x), 1 - y \oplus f(x)\rangle |x\rangle \\ &= |y \oplus f(x)\rangle |x\rangle \end{aligned} \quad (74)$$

We note that the above definition only constrains the states $|x_n, 1 - x_n\rangle$ and $|y, 1 - y\rangle$, where $x_n, y \in \{0, 1\}$. These are only 2 states out of $N + 1$ states per ensemble, hence this clearly leaves a lot of states unspecified. This is in practice not a problem as we will see below, as only linear powers of the total spin operators $S_n^{X,Y,Z}$ are used in the mapping which has the effect of defining the remaining states by linearly interpolating between the definitions.

First considering the constant cases, for $f = 0$ we have from (18)

$$H_{f=0} = 0, \quad (75)$$

where we have chosen the free parameter $j = 0$, as in this approach the assumption is that we are free to choose the most convenient implementation of an oracle. For $f = 1$, since rotations of a single ensemble have identical time coefficients as qubits, this suggests that we have

$$H_{f=1} = \pi \left(\frac{S_0^X - N_0}{2} \right). \quad (76)$$

where we have chosen $2j + 1 = N_0$. While in the qubit case $2j + 1$ is required to be an odd integer, in this case

it is unnecessary and (76) reproduces the desired oracle (74) for any N_0 .

For the balanced cases, the qubit Hamiltonian has the form given in (26). The sum in this expression evaluates to an odd integer if the Hamiltonian operates on a state with $x \in \mathcal{F}$, and an even integer for $x \notin \mathcal{F}$. The oracle thus flips the y -input conditionally on the x -register. This same logic is preserved under the mapping (71), which leads us to the Hamiltonian

$$\begin{aligned} H_f &= \pi \left(\frac{S_0^X - N_0}{2} \right) \\ &\otimes \sum_{x \in \mathcal{F}} (2j_x + 1) \prod_{n=1}^M \frac{1}{2} \left[1 + (-1)^{x_n} \left(\frac{S_n^Z}{N_n} \right) \right]. \end{aligned} \quad (77)$$

Following the same steps as the qubit case to derive the expanded version of the EQC oracle Hamiltonian, we obtain

$$H_f = \pi \left(\frac{S_0^X - N_0}{2} \right) \sum_{z=0}^{2^M-1} \alpha_z \prod_{n=1}^M \left(\frac{S_n^Z}{N_n} \right)^{z_n}. \quad (78)$$

Evolving this Hamiltonian for a time $t = 1$, this satisfies the oracle definition (74). We note that this definition satisfies the constraints of EQC, that the Hamiltonian can be written entirely in terms of linear products of the total spin operator on each ensemble. While we have not yet chosen the free parameters j_x which fix α_z , we shall see in the next section that there is a convenient choice which simultaneously simplifies the implementation and avoids decoherence-prone states.

C. “Quantum” mode operation

Let us now observe what the effect of the oracle is when applied in the Deutsch-Jozsa circuit as shown in Fig. 1(b). The x -register first starts in the state $|0\rangle$, while the y -ensemble starts in the state $|1\rangle$. After the Hadamard gates are applied, the state becomes

$$|\psi_{\text{init}}\rangle = \left| \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}} \right\rangle_0 \prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n. \quad (79)$$

The y -ensemble state is an eigenstate of the S_0^X operator, hence for constant oracles this leave the registers unchanged up to a phase:

$$\begin{aligned} e^{-iH_{f=0}t} |\psi_{\text{init}}\rangle &= |\psi_{\text{init}}\rangle \\ e^{-iH_{f=1}t} |\psi_{\text{init}}\rangle &= (-1)^{N_0} |\psi_{\text{init}}\rangle, \end{aligned} \quad (80)$$

where we evolve for a time $t = 1$.

For the balanced case Hamiltonian, we have (78), or in

expanded form we may write

$$e^{-iH_f t}|\psi_{\text{init}}\rangle = \exp\left[i\pi\left(N_0\alpha_0 + \sum_n \frac{\alpha_n N_0}{N_n} S_n^Z\right.\right. \\ \left.\left.+ \sum_n \sum_{n' \neq n} \frac{\alpha_{nn'} N_0}{N_n N_{n'}} S_n^Z S_{n'}^Z + \dots + \frac{\alpha_{12\dots M} N_0}{\prod_{n=1}^M N_n} \prod_{n=1}^M S_n^Z\right)\right]|\psi_{\text{init}}\rangle \quad (81)$$

where the same steps leading to (29) were performed in this case. It is clear that in the Deutsch-Jozsa circuit, for the constant cases the Hamiltonians leaves the x -register unaffected. Meanwhile, in the balanced cases the Hamiltonian involves a polynomial in S_n^Z operators. In order to distinguish between the constant and balanced cases, what is required is that the S_n^Z terms rotate $|\psi_{\text{init}}\rangle$ sufficiently far away such that it is an orthogonal state. Once it is rotated to an orthogonal state, it should be discriminable via the measurement state at the end of the gate sequence.

To see to what extent the various terms in the expansion (81) take the x -register away from its initial state, let us compute the overlap probability

$$p^{(m)}(\tau) = \left| \langle \psi_{\text{init}} | e^{i\pi\tau \prod_{n=1}^m S_n^Z} | \psi_{\text{init}} \rangle \right|^2. \quad (82)$$

This represents the probability that the initial state $|\psi_{\text{init}}\rangle$ remains in the same state after evolving with various terms in the expansion (81). For balanced Hamiltonians, ideally this is zero such that the final detection probability of $|x=0\rangle$ is zero. Here τ is a parameter which represents the coefficient of $\prod_{n=1}^m S_n^Z$ up to a factor of π . The first few expressions may be evaluated by expanding the coherent states into Fock states, we write the results below:

$$p^{(1)}(\tau) = \cos^{2N_1}(\pi\tau) \quad (83)$$

$$p^{(2)}(\tau) = \frac{1}{4^{N_1}} \left| \sum_{k_1} \binom{N_1}{k_1} \cos^{N_2}[\pi\tau(2k_1 - N_1)] \right|^2 \quad (84)$$

$$p^{(3)}(\tau) = \frac{1}{4^{N_1+N_2}} \left| \sum_{k_1 k_2} \binom{N_1}{k_1} \binom{N_2}{k_2} \right. \\ \left. \times \cos^{N_3}[\pi\tau(2k_1 - N_1)(2k_2 - N_2)] \right|^2. \quad (85)$$

The probabilities are plotted in Fig. 2. We see that all the plots are periodic with period $\tau = 1$. For the qubit case $N = 1$, all curves give the same behavior, where the probability is zero at $\tau = 1/2$. For $N > 1$, in general we see more complex behavior where $p^{(m)}(\tau = 1/2)$ is not necessarily equal to zero. There is a strong even/odd dependence to the curves where qualitatively different behavior is seen for each case. In particular, for N_n all odd the curves have a zero at $\tau = 1/2$, however when even N_n are involved this can instead become 1. For $m \geq 2$ the N_n even cases do not possess a zero at all for any time. The exception to this complex behavior is the

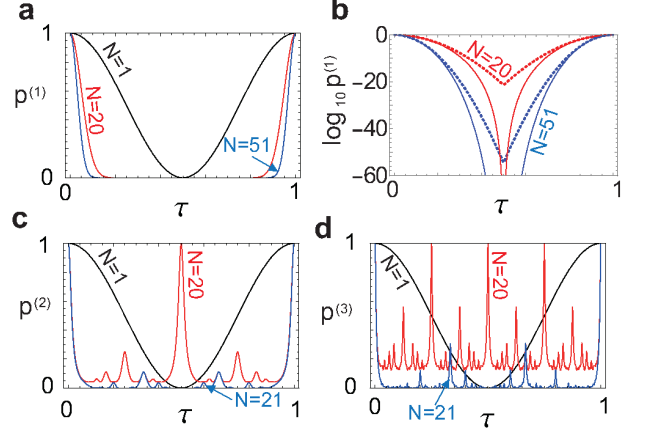


FIG. 2. The probability $p^{(m)}$ of remaining in the initial state $|\psi_{\text{init}}\rangle$ after evolving with a Hamiltonian $\pi \prod_{n=1}^m S_n^Z$, as defined in (82). (a) $m = 1$ with $N_1 = N$ as marked. (b) $m = 1$ on a logarithmic scale with $N_1 = N$ as marked (solid lines), with the approximation (86) (dashed lines). (c) $m = 2$ with $N_1 = N_2 = N$ as marked. (d) $m = 3$ with $N_1 = N_2 = N_3 = N$ as marked.

$m = 1$ case, where there is no even/odd effect, and for any N_1 we have $p^{(1)}(\tau = 1/2) = 0$, as is easily seen from (83). In fact for this case we may approximate for large N_1

$$p^{(1)}(\tau) \approx \sum_j e^{-N_1 \pi^2 (\tau + j)^2}, \quad (86)$$

where j are integers. This approximation is valid in the region where the probability is non-negligible, and $N_1 \gg 1$ as shown Fig. 2(b). Due to the factor of N_1 in the Gaussian, for larger N_1 it is in fact very easy to suppress the overlap probability to zero for the $m = 1$ case. For the qubit case, a time of exactly $\tau = 1/2$ to suppress the probability, whereas for large ensembles we have a window of $1/\sqrt{N_1} \lesssim \tau \lesssim 1 - 1/\sqrt{N_1}$.

This suggests that in terms of minimizing the overlap probability it is most effective to use the $m = 1$ term, as it gives a strong suppression and is most predictable with respect to the number of atoms. The higher order terms would require control of the number of particles in the ensemble to within one atom to control the parity, and is far less desirable. Fortunately, as discussed in Sec. IV A, it is always possible to choose the oracle in a way such that it contains at least one of the $m = 1$ terms with the desired coefficient of $\tau = 1/2$. It is an arbitrary choice of which ensemble to have the $\tau = 1/2$ coefficient, here we shall choose $n = 1$. Returning to the coefficients defined in (29), consider making the choice

$$j_x = -x_1. \quad (87)$$

For this choice the coefficients are

$$\begin{aligned}\alpha_0 &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (-1)^{x_1}, \\ \alpha_n &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (-1)^{x_n + x_1}, \\ \alpha_{nn'} &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (-1)^{x_n + x_{n'} + x_1}, \\ &\vdots \\ \alpha_{12\dots M} &= \frac{1}{2^M} \sum_{x \in \mathcal{F}} (-1)^{\sum_{n=2}^M x_n}.\end{aligned}\quad (88)$$

Specifically, this choice gives

$$\alpha_1 = \frac{1}{2}.\quad (89)$$

Thus by this particular choice of j_x , we have ensured that the coefficient of the S_1^Z term in (81) is equal to

$$-\frac{\pi N_0}{2N_1}.\quad (90)$$

To ensure that the $n = 1$ ensemble in the x -register is orthogonal, this coefficient suggests that we should have $N_0 = N_1$, such that

$$\begin{aligned}e^{i\pi S_1^Z/2} \prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n \\ = e^{-i\pi N_1/2} \left| \frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_1 \prod_{n=2}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle_n,\end{aligned}\quad (91)$$

which has zero overlap with the initial state. However, this is not a very sensitive requirement as for large N_1 the overlap quickly vanishes as seen in Fig. 2(b). Thus

to a reasonable approximation having

$$2\sqrt{N_1} \lesssim N_0 \lesssim 2N_1.\quad (92)$$

should give a sufficiently low overlap state.

The choice (87) fixes the coefficient of S_1^Z , but also affects all the other coefficients (88). How can we be sure that the other coefficients do not spoil the orthogonality that is created by the S_1^Z term? To see this first note that all the terms in (81) commute, so that we may apply any of the terms in any order. Applying the S_1^Z term first, then what we require is that the remaining terms (81) do not somehow make (91) again have an overlap with the initial state $|\psi_{\text{init}}\rangle$. For the other first order $m = 1$ terms, this does not affect the $n = 1$ ensemble, as it they rotate the other coherent states in (91) away from $|\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\rangle$. For the higher order terms $m \geq 2$, we observe that all the coefficients are bounded by

$$|\alpha_z| = \left| \frac{1}{2^M} \sum_{x \in \mathcal{F}} (-1)^{z \cdot x + x_1} \right| \leq \frac{1}{2}.\quad (93)$$

Assuming that all the ensembles are approximately of the same size $N_n \approx N$, then according to (81) the coefficient of an m th order term is

$$\tau \sim \frac{\alpha_z}{N^{m-1}}.\quad (94)$$

Thus for this choice of j_x , the coefficients diminish for higher orders. This suggests that the higher order $m \geq 2$ terms may be negligible, in particular for large N .

To verify this, let us calculate explicitly the effect of whether the higher order terms spoil the orthogonality initially created by S_1^Z . Consider the following probability function which measures how well the orthogonality is preserved after S_1^Z initially creates an orthogonal state:

$$\varepsilon^{(m)}(\tau) = \left| \langle \psi_{\text{init}} | e^{i\pi\tau \prod_{n=1}^m S_n^Z} e^{i\pi S_1^Z/2} | \psi_{\text{init}} \rangle \right|^2.\quad (95)$$

As with (82), we would like this to be as close to zero as possible. This can be evaluated to be

$$\begin{aligned}\varepsilon^{(2)}(\tau) &= \begin{cases} \frac{1}{4^{N_2}} \left| \sum_{k_2=0}^{N_2} \binom{N_2}{k_2} \sin^{N_1} [\pi\tau(2k_2 - N_2)] \right|^2 & \text{if } N_1 \in \text{even} \\ 0 & \text{if } N_1 \in \text{odd} \end{cases} \\ \varepsilon^{(3)}(\tau) &= \begin{cases} \frac{1}{4^{N_2+N_3}} \left| \sum_{k_2=0}^{N_2} \sum_{k_3=0}^{N_3} \binom{N_2}{k_2} \binom{N_3}{k_3} \sin^{N_1} [\pi\tau(2k_2 - N_2)(2k_3 - N_3)] \right|^2 & \text{if } N_1 \in \text{even} \\ 0 & \text{if } N_1 \in \text{odd} \end{cases}\end{aligned}\quad (96)$$

For the case that N_1 has an odd number of particles the probability is exactly zero as the summands in (96) are odd functions. Similarly to $p^{(m)}$, the above functions have a strong dependence on whether the other ensembles

involved have an even or odd number of particles. Fig. 3(a) shows the large timescale behavior for $m = 2$. We see that the functions do possess multiple zeros for both even and odd N_2 , which is in contrast to $p^{(2)}$, where no

zeros are present for even N_1, N_2 . The relevant timescale for our choice of j_x is (94), which we plot in Figs. 3(b)(c). We see that both for the $m = 2$ and $m = 3$ cases the probability remains extremely small, at the $\sim 10^{-7}$ and $\sim 10^{-15}$ levels respectively even for the maximal case where $|\alpha_z| = 1/2$. In Fig. 3(d) we show the particle number dependence of the probability at the maximal case of (94) on a semi-logarithmic plot. The odd/even dependence gives only a minor variation on this scale, and follow a simple exponential form. A fit of the data gives the following estimate of the probability

$$\begin{aligned} \varepsilon^{(2)}\left(-\frac{1}{2N} < \tau < \frac{1}{2N}\right) &\lesssim e^{0.81-0.77N} \\ \varepsilon^{(3)}\left(-\frac{1}{2N^2} < \tau < \frac{1}{2N^2}\right) &\lesssim e^{2.62-1.78N}. \end{aligned} \quad (97)$$

Another source of potential errors is due to the variations in the particle number between the ensembles, which we have so far assumed that $N_n = N$. The effect of different particle numbers in the ensembles is to modify the coefficients in (81). Assuming that the ensembles can be prepared within $\sim 10\%$, this has the effect of shifting τ by this factor, which will generally have the same behavior as (97). A potentially more serious effect is an imperfect rotation of the S_1^Z ensemble, which is the primary source of the desired orthogonality. Such imperfect rotations can be described by

$$\begin{aligned} \varepsilon^{(1)}(\tau) &= \sin^{2N_1}(\pi\tau) \\ &\approx (\pi\tau)^{2N_1} = e^{2\ln(\pi\tau)N_1}. \end{aligned} \quad (98)$$

For ensembles prepared within $\sim 10\%$, this corresponds to an additional rotation of $\tau = 0.05$, which gives an exponent $\varepsilon^{(1)}(\tau) \sim e^{-3.7N}$. This is in fact suppressed more than the error contributions of (97).

We thus conclude that the largest error contribution is $\varepsilon^{(2)}$, due to the second order terms $m = 2$. This is reasonable as these have the largest coefficients after the linear terms, which are the desired terms. In all cases the probability of obtaining the original state is exponentially suppressed with the particle number. In realistic systems the number of particles with $N \gtrsim 10^3$, the above estimates would give an error probability that is completely negligible ($\varepsilon^{(2)} \sim 10^{-334}$). Thus at least in the ideal case, the above shows that it is possible distinguish constant and balanced oracles in the same way as the standard Deutsch-Jozsa algorithm, i.e. by detection, or lack of detection, respectively of $|x = 0\rangle$. While the probability of obtaining $|x = 0\rangle$ is not strictly zero in the balanced case, it is highly suppressed for reasonable parameters, to the extent that it is negligible.

VII. EXAMPLES

In this section we present some explicit examples of EQC implementations of the Deutsch-Jozsa algorithm.

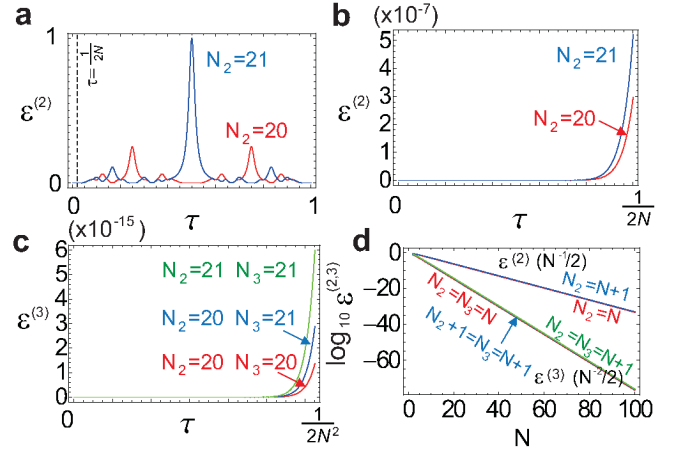


FIG. 3. Error probabilities as defined in (95). This corresponds to the probability for the measurement yielding $|\psi_{\text{init}}\rangle$ for a balanced function for various order terms, after the first order term is applied. (a)(b) The second order error probability $m = 2$ for $N_1 = 20$ and N_2 as marked. (c) The third order error probability $m = 3$, for $N_1 = 20$ and N_2, N_3 as marked. (d) The second $m = 2$ at time $\tau = 1/2N$ and third $m = 3$ error probabilities at time $\tau = 1/2N^2$ as a function of the particle number N . The particle numbers are set as marked, and $N_1 = N$.

A. Deutsch's algorithm

In the case of $M = 1$, the Deutsch-Jozsa algorithm reduces to Deutsch's algorithm. In this case it is in fact possible to use the encoding presented in Sec. VIA to obtain a mapping which works in the EQC framework with negligible error, even for a generalized oracle.

In the case of Deutsch's algorithm, there are only four possible $f(x)$, with two constant and two balanced. The Hamiltonians corresponding to each case are as follows

$$H_{f=0} = 2\pi j \quad (99)$$

$$H_{f=1} = \pi(2j' + 1) \left(\frac{S_0^X - N_0}{2} \right) \quad (100)$$

$$H_{f=\{1,0\}} = \pi(2j_0 + 1) \left(\frac{S_0^X - N_0}{2} \right) \left(\frac{1 + S_1^Z/N_1}{2} \right) \quad (101)$$

$$H_{f=\{0,1\}} = \pi(2j_1 + 1) \left(\frac{S_0^X - N_0}{2} \right) \left(\frac{1 - S_1^Z/N_1}{2} \right) \quad (102)$$

where j, j', j_1, j_0 are integers that may be chosen freely.

For "classical" operation, the above Hamiltonians satisfy the requirements of a valid oracle under the encoding (69) and (70). Evolving the above Hamiltonians for $t = 1$,

and using $S_1^Z/N_1|x\rangle\rangle = (-1)^x|x\rangle\rangle$, we have

$$\begin{aligned} e^{-iH_{f=0}t}|x\rangle\rangle|y\rangle\rangle &= |x\rangle\rangle|y\rangle\rangle \\ e^{-iH_{f=1}t}|x\rangle\rangle|y\rangle\rangle &= |x\rangle\rangle|\bar{y}\rangle\rangle \\ e^{-iH_{f=\{1,0\}}t}|0\rangle\rangle|y\rangle\rangle &= |0\rangle\rangle|\bar{y}\rangle\rangle \\ e^{-iH_{f=\{1,0\}}t}|1\rangle\rangle|y\rangle\rangle &= |1\rangle\rangle|y\rangle\rangle \\ e^{-iH_{f=\{0,1\}}t}|0\rangle\rangle|y\rangle\rangle &= |0\rangle\rangle|y\rangle\rangle \\ e^{-iH_{f=\{0,1\}}t}|1\rangle\rangle|y\rangle\rangle &= |1\rangle\rangle|\bar{y}\rangle\rangle, \end{aligned} \quad (103)$$

where $\bar{y} = 1 - y$ and we have discarded any irrelevant global phase factors.

In “quantum” mode, after the initial Hadamard gates, the Hamiltonian is applied on the state

$$|\psi_{\text{init}}\rangle = \left|\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\rangle_0 \left|\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\rangle_1. \quad (104)$$

For the constant cases, the Hamiltonians clearly leave the ensemble $n = 1$ untouched, so the probability of obtaining $|0\rangle\rangle$ at the measurement is 1. For the balanced cases, the states evolve as

$$\begin{aligned} e^{-iH_{f=\{1,0\}}t}|\psi_{\text{init}}\rangle &= e^{i\frac{N_0\pi(2j_0+1)}{2N_1}S_1^Zt}|\psi_{\text{init}}\rangle \\ &= \left|\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\rangle_0 \left|\frac{e^{i\frac{\pi N_0(2j_0+1)}{2N_1}}}{\sqrt{2}}, \frac{e^{-i\frac{\pi N_0(2j_0+1)}{2N_1}}}{\sqrt{2}}\right\rangle_1 \end{aligned} \quad (105)$$

and

$$\begin{aligned} e^{-iH_{f=\{0,1\}}t}|\psi_{\text{init}}\rangle &= e^{-i\frac{N_0\pi(2j_1+1)}{2N_1}S_1^Zt}|\psi_{\text{init}}\rangle \\ &= \left|\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\rangle_0 \left|\frac{e^{-i\frac{\pi N_0(2j_1+1)}{2N_1}}}{\sqrt{2}}, \frac{e^{i\frac{\pi N_0(2j_1+1)}{2N_1}}}{\sqrt{2}}\right\rangle_1. \end{aligned} \quad (106)$$

The probability of obtaining the initial state is thus

$$\begin{aligned} |\langle\psi_{\text{init}}|e^{-iH_{f=\{1,0\}}t}|\psi_{\text{init}}\rangle|^2 &= \cos^{2N_1}(\pi N_0(2j_0+1)/2N_1) \\ |\langle\psi_{\text{init}}|e^{-iH_{f=\{0,1\}}t}|\psi_{\text{init}}\rangle|^2 &= \cos^{2N_1}(\pi N_0(2j_1+1)/2N_1). \end{aligned} \quad (107)$$

For $N_0 = N_1$, the right hand side evaluates to exactly zero for all j_0, j_1 . For $N_0 \neq N_1$, the probability depends upon the particular choice of free parameters j_0, j_1 . In order to avoid amplifying the particle number mismatch between the ensembles, the safest choice is $j_0 = j_1 = 0$. Assuming that $N_0 \approx N_1$, then in a similar way to (98) we can estimate the probability to be

$$p \sim \left(\frac{\pi(1 - N_0/N_1)}{2}\right)^{2N_1} \quad (108)$$

which is a very small number for typical parameters. For example, for $N_0 = 1000, N_1 = 1100$, one obtains $p \sim 10^{-1863}$, which is negligible. Thus a constant or balanced oracle can be distinguished by a measurement of $|x = 0\rangle\rangle$, in exactly the same way as the qubit version of Deutsch’s algorithm.

B. M=2 case, Method 2

For $M = 2$ there are 6 types of balanced oracles as shown in Table II. Of the balanced oracles, cases 3 and 4 are most non-trivial as they have a dependence on both of the input parameters x_1 and x_2 . For other cases, the functions are independent of one of the variables (for example, $f_1(x)$ is independent of x_1) and give simpler results. Cases 3 and 4 are only different by a global negation, hence we will focus on case 4 – which is the same as that examined in Sec. IV B – for this section.

As seen from (32) and (37), there is not a unique way to realize the oracle corresponding to this (or any) function. In the case that we are allowed to choose the oracle implementation, the simpler choice would be (37), which only involves linear terms in the Pauli operators for the x -register. In this case we would follow the procedure in Sec. VI. The Hamiltonian in this case would be

$$H_{f_4} = \frac{\pi}{2} \left(\frac{S_0^X - N_0}{2} \right) \left(\frac{S_1^Z}{N_1} + \frac{S_2^Z}{N_2} \right). \quad (109)$$

Encoding the logical states as in Sec. VI A, and operating in “classical” mode,

$$e^{-iH_{f_4}t}|y\rangle\rangle|x\rangle\rangle = \begin{cases} |y\rangle\rangle|x\rangle\rangle & x = 1, 2 \\ |\bar{y}\rangle\rangle|x\rangle\rangle & x = 0, 3 \end{cases}, \quad (110)$$

up to an irrelevant global phase. In “quantum” mode, the initial state evolves to

$$e^{-iH_{f_4}t}|\psi_{\text{init}}\rangle = \left|\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\rangle_0 \left|\frac{e^{-i\pi\frac{N_0}{N_1}}}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\rangle_1 \left|\frac{e^{-i\pi\frac{N_0}{N_2}}}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right\rangle_2, \quad (111)$$

which is orthogonal to $|\psi_{\text{init}}\rangle$ for $N_0 = N_1 = N_2$. Similar probability expressions to (107) case can be evaluated.

C. M=2 case, Method 1

Let us also take the approach of Sec. V to implement the $M = 2$ Deutsch-Jozsa algorithm in EQC. One of the drawbacks of this method is that it generates Schrodinger cat states which are vulnerable to decoherence. We calculate the performance under dephasing to analyze the sensitivity of the scheme to decoherence.

Following the exact mapping procedure as discussed in Sec. V, and substituting (44) into (32), we obtain

$$H_{f_4} = \frac{\pi}{4} (S_0^X + N_0) (1 + (S_1^Z + N_1 + 1)(S_2^Z + N_2 + 1)) \quad (112)$$

Operating in “classical” mode, consider evolving the above Hamiltonian on the state (42), which gives

$$\begin{aligned} e^{-iH_{f_4}t}|0, 1\rangle\rangle|k_1 k_2\rangle &= \\ \exp \left[-i\frac{\pi}{2}(S_0^X + N_0)(2k_1 k_2 + k_1 + k_2 + 1) \right] |0, 1\rangle\rangle|k_1 k_2\rangle. \end{aligned} \quad (113)$$

x	x_2	x_1	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
0	0	0	0	0	0	1	1	1
1	0	1	0	1	1	0	0	1
2	1	0	1	0	1	0	1	0
3	1	1	1	1	0	1	0	0

TABLE II. Balanced Deutsch-Jozsa functions for $M = 2$.

The factor $2k_1k_2 + k_1 + k_2 + 1$ can be observed to be an odd integer when both k_1 and k_2 are odd or even, and is an even integer when one of k_1 and k_2 are odd. Thus the same form as (54) is obtained, where only the $x = 0$ and $x = 3$ cases rotate the y -ensemble:

$$e^{-iH_{f_4}t}|0, 1\rangle\rangle|k_1k_2\rangle = \begin{cases} |0, 1\rangle\rangle|k_1k_2\rangle & k_1, k_2 \leftrightarrow x = 1, 2 \\ |1, 0\rangle\rangle|k_1k_2\rangle & k_1, k_2 \leftrightarrow x = 0, 3 \end{cases}. \quad (114)$$

In “quantum” mode, after the Hadamard gates the initial state is (58), which in this case we write

$$|\psi_{\text{init}}\rangle = |k_0\rangle_x \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle. \quad (115)$$

Operating on this state, the state is

$$\begin{aligned} & e^{-iH_{f_4}t}|\psi_{\text{init}}\rangle \\ &= \frac{1}{2} \exp \left[-i\frac{\pi}{2}k_0 (1 + (S_1^Z + N_1 + 1)(S_2^Z + N_2 + 1)) \right] \\ &\times |k_0\rangle_x \left(|+\rangle\rangle|+\rangle\rangle + |+\rangle\rangle|-\rangle\rangle + |-\rangle\rangle|+\rangle\rangle + |-\rangle\rangle|-\rangle\rangle \right), \end{aligned} \quad (116)$$

where we have used the even and odd Schrodinger cat definitions of (62) and (63). Since $|+\rangle\rangle$ only contains even $|k\rangle$ Fock states, and $|-\rangle\rangle$ contains odd $|k\rangle$ Fock states, according to the same argument as (113), the $|+\rangle\rangle|+\rangle\rangle$ and $|-\rangle\rangle|-\rangle\rangle$ terms pick up a factor of -1 , while the other terms remain the same. The state thus becomes

$$\begin{aligned} e^{-iH_{f_4}t}|\psi_{\text{init}}\rangle &= -|k_0\rangle_x \frac{1}{2} (|+\rangle\rangle - |-\rangle\rangle) (|+\rangle\rangle - |-\rangle\rangle) \\ &= -|k_0\rangle_x \left| \frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle \left| \frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle. \end{aligned} \quad (117)$$

The above state has zero overlap with the initial state $|\psi_{\text{init}}\rangle$, which shows that in the ideal case this reproduces the Deutsch-Jozsa algorithm.

Now let us introduce decoherence in the form of dephasing, which has a master equation [15, 16]

$$\frac{d\rho}{dt} = -\frac{\Gamma}{2} \sum_{n=1}^M ((S_n^Z)^2 \rho - 2S_n^Z \rho S_n^Z + \rho (S_n^Z)^2) \quad (118)$$

where Γ is the dephasing rate. For simplicity we ignore the dephasing on the y -ensemble, as this takes a passive role operating in “quantum” mode. The dephasing has the effect diminishing the off-diagonal terms

$$\rho_{k_1 \dots k_M k'_1 \dots k'_M}(t) = \rho_{k_1 \dots k_M k'_1 \dots k'_M}(0) e^{-2\Gamma t \sum_{n=1}^M (k_n - k'_n)^2},$$

where $\rho(0)$ is the initial state and $\rho_{k_1 \dots k_M k'_1 \dots k'_M} = \langle k_1 \dots k_M | \rho | k'_1 \dots k'_M \rangle$.

In an experiment the observables are typically expectation values of the spin operators $\langle S_n^{X,Y,Z} \rangle$. As our aim is to distinguish between states where the state is preserved in $|\psi_{\text{init}}\rangle$ (constant functions) and deviating from $|\psi_{\text{init}}\rangle$ (balanced functions), we define a signal quantity with respect to the initial state according to

$$\mathcal{S} = \prod_{n=1}^M \frac{1}{2} \left(1 + \frac{\langle S_n^Z \rangle}{N_n} \right). \quad (119)$$

where the expectation value is taken for the state at the end of the full gate sequence in Fig. 1(b). We can equally write the signal as

$$\mathcal{S} = \prod_{n=1}^M \frac{1}{2} \left(1 + \frac{\langle S_n^X \rangle'}{N_n} \right), \quad (120)$$

where the state is taken to be immediately after the oracle. For the constant cases, in the ideal case $\langle S_n^Z \rangle / N_n = 1$ and we obtain $\mathcal{S} = 1$. For the balanced cases, in the ideal case, in (68) all the terms give at least one spin where $\langle S_n^Z \rangle / N_n = -1$, which immediately gives $\mathcal{S} = 0$. This quantity may thus be used to distinguish between the constant and balanced cases.

Let us examine what happens to the signal for each of the cases under the presence of decoherence, assumed to be present primarily during the oracle evaluation. In the constant case, $|\psi_{\text{init}}\rangle$ remains unchanged due to the oracle. Hence the only change that will occur to the x -register in this case is the dephasing. The initial density matrix is thus

$$\rho(0) = \prod_{n=1}^M \left| \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right\rangle \left\langle \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right|. \quad (121)$$

It is possible to evaluate exactly the time evolution under the master equation in this case, and we have

$$\langle S_n^X \rangle' = N_n e^{-2\Gamma t}. \quad (122)$$

The signal behaves as

$$\mathcal{S}_{\text{constant}} = \left[\frac{1}{2} (1 + e^{-2\Gamma t}) \right]^M \approx 1 - \Gamma M t, \quad (123)$$

where we have assumed $N_n = N$ for simplicity. Note that there is no dependence on N for the signal, which shows

that the same performance for macroscopic samples with large N are obtained as for qubits $N = 1$. The initial decay of the signal has a characteristic time $t \sim 1/\Gamma M$, which shows the signal is of the order of the dephasing time.

For the balanced cases, we expect that the emergence of Schrodinger cat states will be very quickly destroyed into mixed states. For example, for an initial state such as $\frac{1}{\sqrt{2}}(|1, 0\rangle + |0, 1\rangle)$, the density matrix decays as

$$\begin{aligned} \rho(t) = & \frac{1}{2} \left(|1, 0\rangle\langle 1, 0| + |0, 1\rangle\langle 0, 1| \right. \\ & \left. + e^{-2N^2\Gamma t} |1, 0\rangle\langle 0, 1| + e^{-2N^2\Gamma t} |0, 1\rangle\langle 1, 0| \right) \end{aligned} \quad (124)$$

which have off-diagonal terms that decay very quickly. This will be true for states such as (68), which is in general an entangled state involving Schrodinger cats. In these cases, we would typically obtain a mixed state with expectations $\langle S_n^Z \rangle / N_n \rightarrow 0$. Substituting into (119), we expect the signal in these cases to be

$$\mathcal{S}_{\text{balanced}} \approx \frac{1}{2^M}. \quad (125)$$

Comparing (123) and (125), we see that as long as $\Gamma M t \ll 1$, it is possible to clearly distinguish between the constant and balanced cases, despite the presence of decoherence. The reason for this is the fortuitous difference in the nature of the states in the balanced and constant cases. In the constant cases, the states are untouched, hence the states remain spin coherent states, which are relatively stable states even in the presence of decoherence. Meanwhile, for the balanced cases, potentially decoherence-prone Schrodinger cat states are generated, which under decoherence evolve quickly to mixed states. However, since the aim is to create a different state to the initial state, this mixed state is sufficient for detection of a balanced function. Thus while the decoherence indeed deteriorate the signal from the ideal value of $\mathcal{S} = 0$ to $\mathcal{S} = 1/2^M$, it does not do so in a catastrophic way. Due to the nature of the detection of the Deutsch-Jozsa algorithm, despite the generation of fragile Schrodinger cat states, this allows for the detection to distinguish between the two cases. Naturally this does not change the fact that Fock states need to be prepared for Method 1, which may be difficult in practice. Thus Method 2 may be the approach of choice for these considerations.

VIII. SUMMARY AND CONCLUSIONS

We have presented two methods of mapping the Deutsch-Jozsa algorithm, as originally formulated for qubits, onto implementations using ensembles of qubits. We follow the EQC framework developed previously such that only Hamiltonians involving linear products of total spin operators are used, and collective measurements

are made. In either of the two methods, the number of times the oracle needs to be executed is one, precisely the same as for the qubit case. This provides an exponential quantum speedup over the classical case where at least half the input combinations must be tested. The resource counts for the remaining part of the Deutsch-Jozsa algorithm is also the same, counting the resource for executing a Hadamard gate the same as for a qubit and ensemble.

The two methods presented provide two different encodings for storing qubit information. In Method 1, the binary information is stored as the parity of the Fock states. The advantage of this approach is that it can map an arbitrary Deutsch-Jozsa oracle onto the EQC framework. The Deutsch-Jozsa oracle can be implemented using an infinite number of different Hamiltonians, and the approach is suitable if this generality is required in the mapping. The drawback of Method 1 is that Schrodinger cat states are generated by the oracle, which are prone to decoherence. However, as discussed in Sec. VII C, due to the nature of the measurement discrimination between constant and balanced cases, in practice a clear signal difference should nevertheless be obtained between the two cases. The reason for this is that to distinguish between the two cases, all that is required is a significant deviation from the initial state in the balanced case, which is realized even when decoherence is present.

In Method 2, an encoding corresponding to orthogonal spin coherent states on the Bloch sphere was used. This encoding cannot map all qubit oracle realizations, hence does not have the generality of Method 1. It nonetheless can realize any of the $\binom{2^M}{2^M-1}$ balanced and the two constant functions. Hence the reduction in generality is only in the degrees of freedom allowed in the oracle realization, and not a restriction of the algorithm itself. In this case, the algorithm works only to finite probability, hence is an approximation to the qubit case. While approximate, the dominant errors are exponentially suppressed $\sim e^{-0.77N}$, hence in practice the errors are negligible for large ensemble sizes.

This paper has shown that it is possible to perform the Deutsch-Jozsa using macroscopic ensembles under the practical restrictions imposed by EQC. This joins the other quantum algorithms that are possible under EQC, namely quantum teleportation [16, 17] and Deutsch's algorithm [15]. Our results also reproduce the results already found for Deutsch's algorithm under a more general setting. In the current work, our aim was simply to reproduce the results of the qubit version of the algorithm faithfully. One advantage of using ensembles is that it is possible – unlike qubits – to read out using non-destructive means the state of a spin coherent state [26]. Such features are not utilized in this or the other quantum algorithms that have been mapped successfully from qubits. Utilizing such non-destructive measurements has the potential to lead to other quantum algorithms in EQC that are not possible with qubits.

ACKNOWLEDGMENTS

This work is supported by the Shanghai Research Challenge Fund, New York University Global Seed Grants for Collaborative Research, National Natural Science Foundation of China grant 61571301, and the Thousand Talents Program for Distinguished Young Scholars.

-
- [1] D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985).
 - [2] D. Deutsch and R. Jozsa, Proc. R. Soc. London A **439**, 553 (1992).
 - [3] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. R. Soc. London A **454**, 339 (1998).
 - [4] L. K. Grover, in *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing* (ACM, New York, NY, USA, 1996), STOC '96, pp. 212–219, ISBN 0-89791-785-5, URL <http://doi.acm.org/10.1145/237814.237866>.
 - [5] P. W. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 1994), SFCS '94, pp. 124–134, ISBN 0-8186-6580-7, URL <http://dx.doi.org/10.1109/SFCS.1994.365700>.
 - [6] D. Collins, K. W. Kim, W. C. Holton, H. Sierzputowska-Gracz, and E. O. Stejskal, Phys. Rev. A **62**, 022304 (2000).
 - [7] Z. Wu, J. Li, W. Zheng, J. Luo, M. Feng, and X. Peng, Phys. Rev. A **84**, 042312 (2011).
 - [8] N. Schuch and J. Siewert, Phys. Stat. Sol. (b) **233**, 482489 (2002).
 - [9] S. Takeuchi, Phys. Rev. A **62**, 032301 (2000).
 - [10] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, Nature **421**, 48 (2003).
 - [11] S. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
 - [12] B. Julsgaard, A. Kozhekin, and E. S. Polzik, Nature **413**, 400 (2001).
 - [13] H. Krauter, D. Salart, C. A. Muschik, J. M. Petersen, H. Shen, T. Fernholz, and E. S. Polzik, Nature Phys. **9**, 400 (2012).
 - [14] T. Byrnes, K. Wen, and Y. Yamamoto, Phys. Rev. A **85**, 040306 (2012).
 - [15] T. Byrnes, D. Rosseau, M. Khosla, A. Pyrkov, A. Thomasen, T. Mukai, S. Koyama, A. Abdelrahman, and E. Ilo-Okeke, Opt. Comm. **337**, 102 (2015).
 - [16] A. N. Pyrkov and T. Byrnes, New J. Phys. **16**, 073038 (2014).
 - [17] A. N. Pyrkov and T. Byrnes, Phys. Rev. A **90**, 062336 (2014).
 - [18] P. Bohi, M. F. Riedel, J. Hoffrogge, J. Reichel, T. W. Hansch, and P. Treutlein, Nature Phys. **5**, 592 (2009).
 - [19] M. F. Riedel, P. Bohi, Y. Li, T. W. Hansch, A. Sinatra, and P. Treutlein, Nature **464**, 1170 (2010).
 - [20] A. Pyrkov and T. Byrnes, New J. Phys. **15**, 093019 (2013).
 - [21] M. I. Hussain, E. O. Ilo-Okeke, and T. Byrnes, Phys. Rev. A **89**, 053607 (2014).
 - [22] A. Abdelrahman, T. Mukai, H. Häffner, and T. Byrnes, Opt. Express **22**, 3501 (2014).
 - [23] T. Byrnes, Phys. Rev. A **88**, 023609 (2013).
 - [24] H. Kurkjian, K. Pawowski, A. Sinatra, and P. Treutlein, Phys. Rev. A **88**, 043605 (2013).
 - [25] T. Byrnes, D. Rosseau, M. Khosla, A. Pyrkov, A. Thomasen, T. Mukai, S. Koyama, A. Abdelrahman, and E. Ilo-Okeke, Opt. Comm. **337**, 102 (2014).
 - [26] E. O. Ilo-Okeke and T. Byrnes, Phys. Rev. Lett. **112**, 233602 (2014).
 - [27] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, New York, 2000).